RF and Network Signature-Based Machine Learning on Detection of Wireless controlled Drone

Teoh, Yan Jun John[1], **Seow Chee Kiat**[2]

[1]University of Glasgow, United Kingdom
[2]University of Glasgow, United Kingdom

Abstract— Over the years, drone usage have become an increasing part of the ever-connected society that we are currently living in. Its usages have proliferated beyond the military sector to various commercial and consumer activities such as package delivery, disaster relief, agriculture and filming. Wi-Fi controlled drone has increased its popularity for personal use due to its affordability, and the ease of operating the drone through smart-devices like mobile phone, tablets and computers. As such, this increases the likelihood of drone presence in various environments, especially in critical government infrastructure, leading to various privacy and security concern by the authorities and the public with malicious intent. Therefore, various signature-based methodology of drone detection has emerged such as the visual and Radio Frequency (RF) signature-based detection method. Visual signature-based detection relies on camera capture and image processing but this is an expensive approach. Whereas, RF signature-based detection relies on the identification of the emission of RF signal by the drone. However, since most commercial electronics devices were built based on Wi-Fi technology, the differentiation of the RF signals transmitted between a drone or a standard Wi-Fi device in a crowded Wi-Fi environment such as a school campus or city area is a challenging task.

In this paper, we propose a novel Machine Learning (ML) approach that leverages on both RF and network packets measurement to identify the presence of Wi-Fi drone in an urban setting. These two measurements were jointly analyzed to create unique signatures to differentiate a Wi-Fi drone and a standard Wi-Fi device. Furthermore, we also propose a meticulous pre-processing procedure and a better training scheme of using Stratified K-Fold Cross-Validation (SKFCV), to enhance the richness in the data signature and fully exploit the permutation of the data during training respectively for better performance of the ML models. Two supervised classification ML models, namely the Logistic Regression (LR), and Artificial Neural Network (ANN) were applied using the joint data measurements to identify the presence of drone in dense Wi-Fi environment. The experimental results have shown that the proposed novel ML approach of using both RF and network measurement signatures coupled with the pre-processing and training methodology on LR and ANN ML models have outperformed the traditional RF signature-based drone detection ML accuracy results by 15.1% and 21.63% respectively in a crowded Wi-Fi environment.

1. INTRODUCTION

Network connectivity was initially seen as an optional commodity, but now it is considered an essential utility. An ever growing number of smart devices that needs to be continuously connected to the network because of the advent of the Internet of Things (IoT) paradigm. Many Wi-Fi drones these days can operate through smart devices to avoid interference or interception of other drone's commands, and certain Remote Controllers (RC) are enabled with either Direct-Sequence Spread Spectrum (DSSS) or Frequency-Hopping Spread Spectrum (FHSS) to hide the transmissions within the noise floor of the RF spectrum. Thus, with the capability and convenience that Wi-Fi drones can deliver, it has become a popular product among the consumer market, and potential threats from drones may arise when flying in unauthorised areas.

With the threat of drones increasing, there are various anti-drone systems proposed by experts today to combat against these threats. One method is to deceive the rogue drone's localization system by spoofing the global positioning system (GPS) signals [1]. Another method involves the spoofing of RF signals of the drone remote controls (RC) to disrupt drone operations [2]. However, even with such anti-drone systems put in place, detecting a drone presence in an urban setting remains a challenge. One of the most prominent challenges in detecting drone presence today is to differentiate the RF and network signatures between a standard Wi-Fi device and a Wi-Fi operating drone. Both devices may display similar traits of signatures, in terms of Received Signal Strength (RSS) in the RF spectrum and the network packets transmitted over the Wi-Fi

network. In addition, the network configuration of these devices is configurable to hide its Service Set Identifier (SSID) or Media Access Control (MAC) address, which prevents accessible software tools like the Wi-Fi scanner to detect the network and capture the network details of the devices. Thus, any rogue drone operator could easily exploit these vulnerabilities to set their drone to stay hidden over the RF or the network spectrum and perform an illegal flying operation.

Existing drone detection techniques include:

- Based on RF signatures using spectrum analyzer [3, 4, 5], inexpensive Commercial Off-The-Shelf (COTS) technology approaches such as the use of Wi-Fi receivers and Software Defined Radios (SDR) have been used to detect the drone but although inexpensive, detection accuracy is always in doubt due to similarity in RF signature.

- Based on different localization methodology [6, 7, 8, 9], detection of the drone can be effective but inaccurate in estimating the drone location.

- Based on network signatures using network packets sniffing tool [10, 11], has proven to achieve good accuracy in identifying drone presence and its type. However, it only applies to specific drone models.

- Based on ML methods [3, 10] where ML method [3] identifies drone through training with RF measurements using isolated drone signals but it may not be accurate in detection when Wi-Fi devices emit similar signals as the drone. On the other hand, literature [10] uses multiple machine learning classifier and trained with network-based measurements. The results display better performance in differentiating the devices in a crowded Wi-Fi environment. Although this approach demonstrates excellent performance in detecting Wi-Fi drone presence, its accuracy remains to be improved.

In this paper, a novel ML method of using both RF and network-signature measurements with two ML classifiers in order to detect the presence of drone in a crowded Wi-Fi environment is proposed. In addition, a pre-processing data methodology, together with SKFCV training scheme was devised to enhance the performance of the detection models. Firstly, an overview of the process flow will be covered in the Section 2. This is followed by an elaboration of the two drone detection techniques that were applied to differentiate the drone presence in Section 3. Section 4 covers the illustration of the data collection process followed by meticulous pre-processing steps of the data and the training scheme for the ML classifiers, namely Logistic Regression and Artificial Neural Network[12]. Lastly, the results of each classifier and comparison with existing RF-based classifier performance [3] for drone detection will be presented in Section 5 and conclude in Section 6.

2. OVERVIEW OF METHODOLOGY

This section covers an overview of the process flow in achieving the proposed approach results.

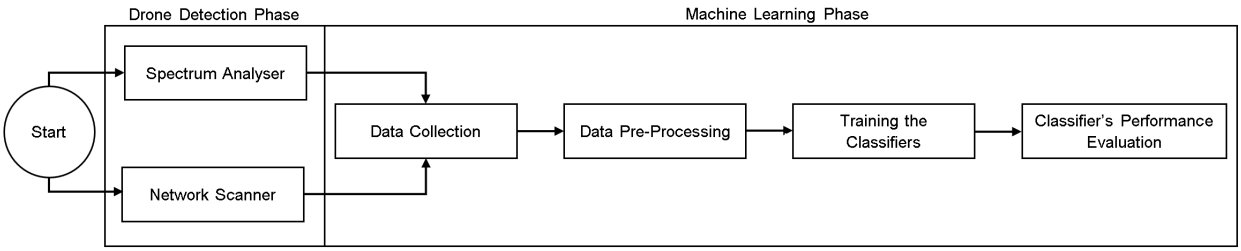


Figure 1: Process Flow

As shown in figure 1, the process involves two phases. The first phase begins with the drone detection to identify the drone signatures in a dense Wi-Fi area. It is followed by the processes of implementing the ML classifiers for drone detection. This process flow will be further articulated in Section 3 and 4.

3. DRONE DETECTION PHASE

Drone detection experiments were conducted to collect and analyze both the Wi-Fi drone and the standard Wi-Fi devices signature characteristics using both RF and network data detection techniques.

Figure 2: Experimental Tools

3.1. Spectrum analyzer

In this RF detection experiment, a low-cost Software Defined Radio (SDR) known as HackRF One by Great Scott Gadgets was used as a Radio Frequency receiver and paired with the HackRF Sweep Spectrum analyzer (HSSA) software to scan and analyze the RF signatures in the Wi-Fi RF spectrum. The SDR is capable of receiving RF signals from a range of 1 MHz to 6 GHz. Hence, it could receive RF signals from the Wi-Fi ISM 802.11x bandwidth of 2.4GHz-2.5GHz. In addition, a popular Wi-Fi drone model Mavic Air, operated using a smartphone, was utilized as shown in figure 2.

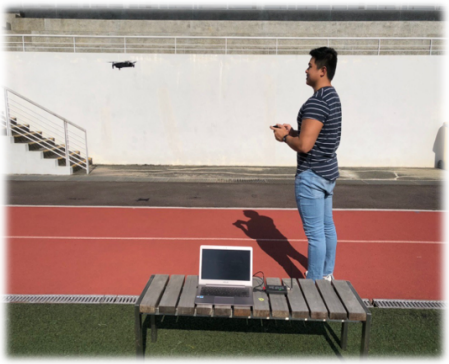


Figure 3: Spectrum analyzer Conduct

The experiment was conducted in an open area of the school campus to simulate a crowded Wi-Fi environment as shown in figure 3. The Mavic Air was preset to a specific Wi-Fi channel in order to identify the drone signatures in the spectrum. During the drone flight, all the controls of the drone, including video and photo capturing were utilized, so that the observation of the transmitted signals pattern could be analyzed to study the device signatures.

The observed RF signatures from HSSA shows that the Mavic Air signature displays a higher RSS that fluctuating over time as compared to the other Wi-Fi devices around the area. This is due to the fact that the drone is flying nearer to the receiving range of the SDR as compared to the stationary Wi-Fi devices around the building compound which was far away from the receiver. However, when an additional mobile device creates a hotspot network with the same RF channel as the drone, the RSS transmission becomes hard to differentiate whether the transmitted signature was from which devices.

A simple spectrum analyzer detection technique could only estimate the probability of a drone presence. Thus, inspecting the network signature could aid in enhancing the prediction of a drone presence more accurately.

3.2. Network Scanner With Packets Sniffing Tools

The same experimental set-up and experiment flow were used for this network detection experiment with an add-on of using the Wi-Fi Scanner and network packet sniffing software tool to capture the network signatures. For this experiment, the Mavic Air Wi-Fi network must be made known in order for the software to detect and capture the drone network signature. Also, a ten-minutes timeframe for this experiment was adhered to observe the network communication pattern and collect more data samples of the Wi-Fi devices around the area.

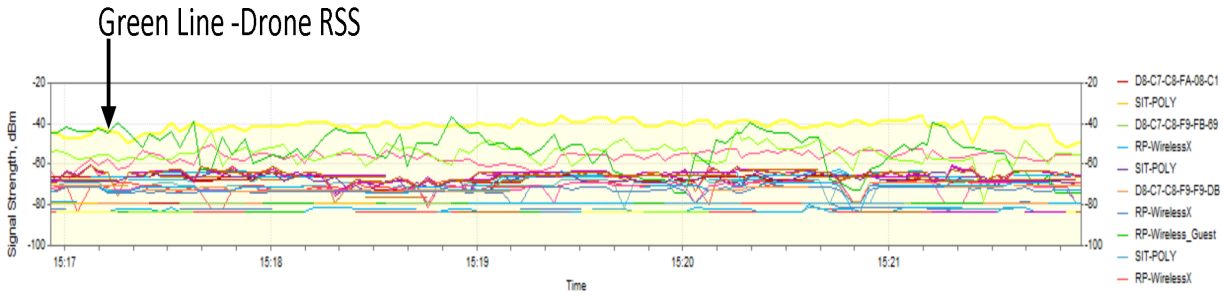


Figure 4: Wi-Fi Scanner RSS

As shown in figure 4, the software was able to display the RSS pattern over the first five-minutes timeframe, and the captured signatures using Wi-Fi scanner is aligned with the HackRF spectrum analyzer readings. This illustrates that the RSS of a drone would be fluctuating over time with higher RSS if it is flying around the area as compared to the standard Wi-Fi devices RSS, which remain relatively constant.

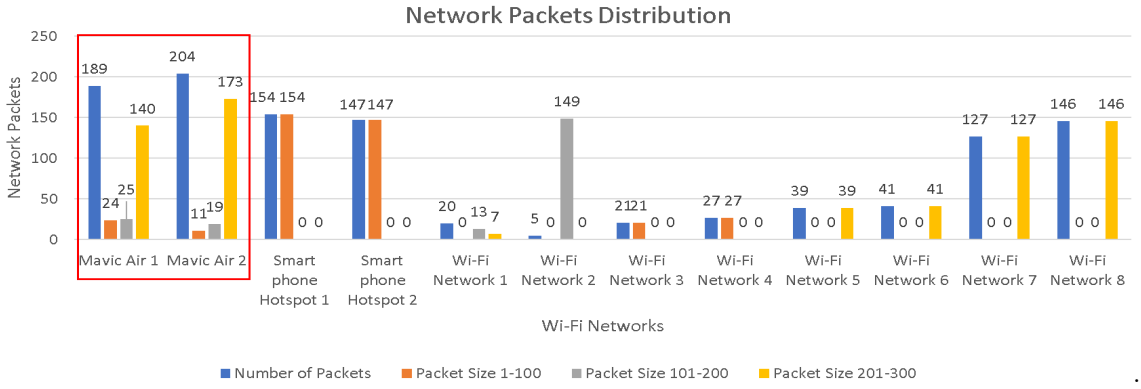


Figure 5: Network Packets Distribution

At the end of ten-minutes timeframe, the captured network data was exported out as a CSV file to examine the difference in the network packets characteristics of the Wi-Fi devices as shown in figure 5. Through inspection, the characteristics observed have shown the proven study by Nguyen et al. that the drone network packets transmitted number was higher than the other Wi-Fi devices, and the majority of the transmitted packet is more significant in size [5].

Therefore, the experiments have proven using both RF and network detection techniques jointly could be used as a useful low-cost tool in identifying the presence of a Wi-Fi operating drone in a dense Wi-Fi area.

4. MACHINE LEARNING PHASE

In this section, the proposed machine learning approach for drone detection in Wi-Fi networks will be illustrated.

4.1. Data Collection

Figure 6 illustrates the data collection process set-up which simulated to a real-world scenario when a drone presence occurred.

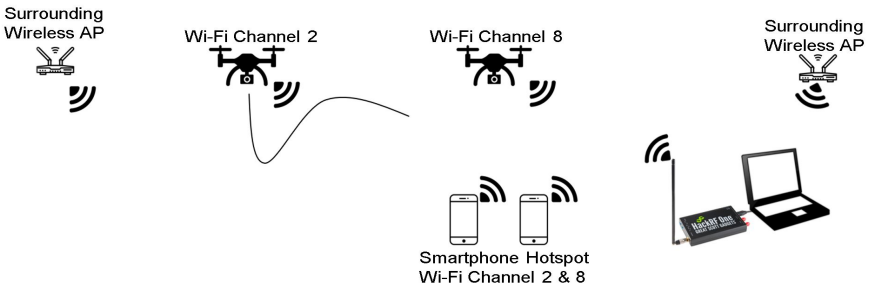


Figure 6: Data Collection Set-Up

Two Mavic Air drone models were used, where one drone would be simulating to fly around the area, and the other drone would remain stationary. Furthermore, the hotspot network of the two smartphones devices was turned on and placed near the SDR. The purpose of this set-up was to use the smartphone to overlap its signatures with the operated drones so that the collected data measurements would have certain similarities between the drone data and the Wi-Fi devices.

During the data collection, the HackRF_sweep command and network packets scanner were employed. The sweep command "HackRF_sweep -f 2400:2490 > datafile.csv" instructs the HackRF to scan within a certain frequency range and output its scan into a CSV file. The network packets scanner was enabled in the Acrylic Wi-Fi software and can be exported out into a CSV file as well. Both the sweeping of RF and network signatures were captured at the same time for a duration of ten-minutes timeframe so that the readings from both data files can be matched and there would be sufficient amount of data to train the ML classifiers.

In addition, a new set of data measurement will be collected as test data, using a similar simulated scenario as the first data collection conduct with a slight modification. The modification includes the change in the operating Wi-Fi channels for the two drones. This test data will then used to evaluate the trained classifiers and observed whether if the classifiers will then be able to achieve good prediction of differentiating the drones under different conditions.

4.2. Feature Selection and Labelling

Feature selection is an essential process of the ML procedure. With adequate amount of features selected in the data file, it could minimize the problem in over-fitting the trained ML classifiers that can lead to bad prediction performance. Hence, feature selection for the data files is essential in prevention of such occurrence.

Based on the observation made from the experiments, signatures such as the frequency range, signal strength, number of network packet and size were used as the distinct data features to differentiate the presence of drone from the standard Wi-Fi devices. Henceforth, these features were selected as the finalized data features for training the classifiers.

The finalized data file was modified to add a column, namely "Drone Detected" to indicate the binary classification for the classifiers as the target variable. The data was filtered according to the identified signatures and marked with "1" for each row that was classified as drone and "0" for a standard Wi-Fi device.

4.3. Data Pre-Processing

During the pre-processing data stage, the finalized data file was cleaned by removing all collected RF signatures that have missing network data inputs. The purpose was to remove all the unnecessary noise in the data as these data rows have no relation with the detected Wi-Fi devices, which does not aid in the differentiation of the drone presence by the ML classifiers.

The next step involves the scaling of the data features. Feature scaling through standardization is an important pre-processing step for many machine learning algorithms, especially for classifiers like LR and ANN. The standardization using standard scores which is also called z scores of the samples follow a Gaussian distribution formula as follows:

$$z = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{1}$$

where μ and σ are the expectation and the standard deviation of the distribution. The purpose is to rescale each feature to be Gaussian distributed with a mean of zero and a standard deviation

of one so that when the data is fit into the classifiers, it can train faster and have better accuracy performance. As such, the whole data set assumes multivariate Gaussian distribution.

4.4. Training Scheme For The Classifiers

The conventional approach of training the ML classifiers is to split the data file into a specific ratio of training and testing data set. The training data would be used to fit into the classifier for training and the test data will be used to evaluate against the trained performance of the classifier. However, this approach of splitting the data could result in an imbalance of target variable classes in the split data sets. It will result in a trained classifier that would be poor in estimation and prediction of the desired output.

In this paper, SKFCV technique for both classifiers with an additional hyperparameter tuning scheme implemented for the ANN classifier [13], which is known as Grid Search Cross-Validation (GSCV) are used to overcome the imbalance issue.

SKFCV is an enhancement of a K-Fold cross-validation technique, wherein K-Folds cross-validation splits the data into k different subsets and use *k-1* subsets to train our data and leave the last subset as validate data. With stratification, it helps the K-Fold CV to ensure these split subsets are arranged in such a way that each class comprises around half the instances in each fold, so that each subset is a good representative of the original data during training. Averaging over all folds is then used to obtain the finalized classifier which would be used to test against the testing data set.

In addition of using SKFCV to achieve balance in data split, GSCV is used to tune the ANN parameters to obtain the best parameters to achieve good performance and computation time. The parameters are the number of the epoch, batch size, neurons and hidden layers to be utilized for the classifiers. The best obtained parameters were then used in the prediction of output in the testing data set.

4.5. Machine Learning Model Selection

The selection of the ML model is always a tradeoff between complexity and performance. A complex classifier may require higher resource consumption but is likely to return a significant good performance if it is properly trained, whereas a simple model may provide adequate performance while consuming fewer resources. In this paper, the following supervised classification machine learning models were evaluated and this evaluation will assist to decide whether a simplex or a complex model will be suitable to solve the problem.

Logistic Regression is a specific type of Generalised Linear Model (GLM). Unlike other regression models, it is a classification method algorithm used to determine the probability of an outcome (target variable) in binary number "0" or "1" based on the sigmoid equation

$$p = \frac{1}{1 + e^{-(\alpha+\beta_1 x_1+...+\beta_n x_n)}} \tag{2}$$

where x_1 to x_n are features used for fitting into the LR classifier, and α, β_1 to β_n are parameters of the classifier. In the context of this paper, the target variable was categorised into two categories: "1" drone detected and "0" otherwise.

ANN was part of the deep learning models and could be used to solve different types of problems other than classification or regression. However, in this paper, ANN is used as a classifier in solving the detection of drone presence. The architecture of this algorithm involves different layers component to derive the desired results. In figure 7, the ANN architecture and process flow of the implementation is shown.

- The input layer: comprises several input neurons where each neuron represents a feature in the dataset. It takes the inputs and passes them to the next layer.
- The hidden layer: is found in between the input layers and output layers, where the neurons in this layer will take in a set of weighted inputs from the previous layer and produce an output through a selected Activation Function (AF). The utilized AF Rectified Linear units (ReLu) which were widely used AF in many deep learning models produced better performance and generalisation in deep learning applications as compared to other activation functions, such as Sigmoid and Tanh [14]. In the equation, the max input value is taken and pass as the output value z.

$$Relu(x) = max(0, x) \begin{cases} 0, if x < 0 \\ x, if x \geq 0 \end{cases} \tag{3}$$

- The output layer: it is similar to hidden layer except it gives the final result of the ANN architecture, wherein this paper context, it is a binary value output for classification of Wi-Fi drones and standard Wi-Fi devices by using the sigmoid function.

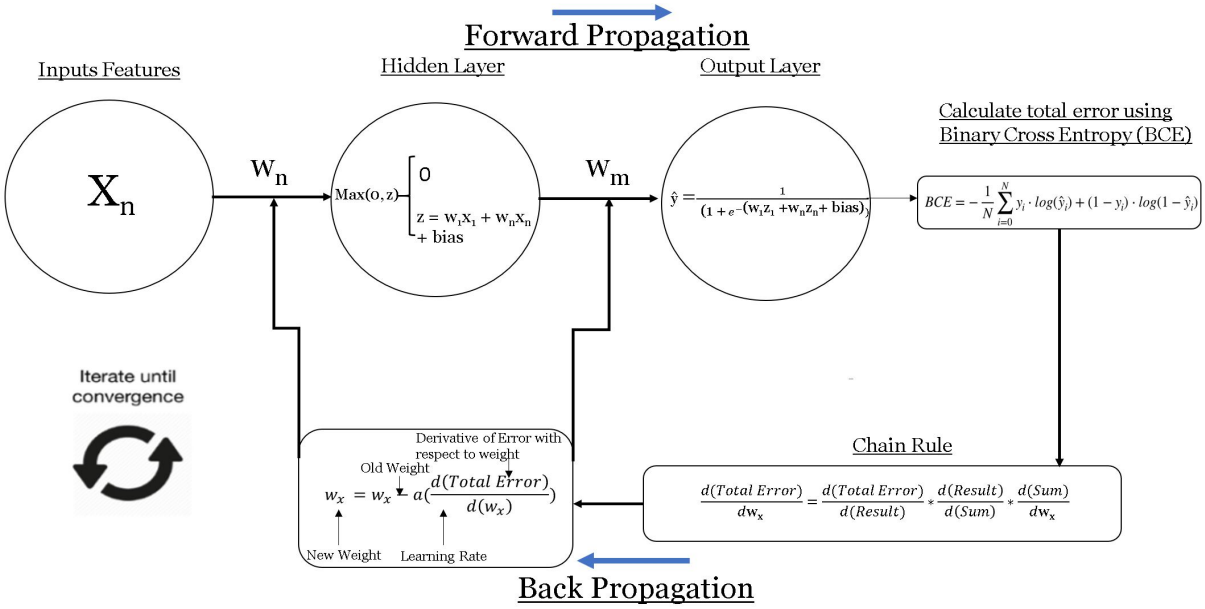


Figure 7: Artificial Neural Network Architecture With Forward and Back Propagation Flow

The implementation process of ANN comprises of two components: Forward-propagation and backward propagation. Forward propagation is a process flow of ANN to feed the feature inputs through the neural network in a forward direction and produce the result of the prediction at the output layer. As for the back-propagation process, it involves taking in the loss error value for classification which is calculated using Binary Cross Entropy (BCE).

$$BCE = -\frac{1}{N}\sum_{i=1}^{N} y_i \cdot log(\hat{y}_i) + (1 - y_i) \cdot log(1 - \hat{y}_i) \tag{4}$$

where N is the total observations in the data set. y_i and $\hat{y}_i$ are the actual binary value class label of either "1" or "0" arising from i^{th} dataset and its predicted sigmoid function probability at the neuron output layer respectively. BCE value is applied at the chain rule formula to calculate the derivative of error with respect to weight, where the result and the sum are the output and the aggregate function for a particular neuron respectively at either in the hidden or output layer.w_x is the weight to be calculated. The primary goal of the back-propagation is to take the new weights w_x to update new values of weights for w_n and w_m respectively in the network, and allow the predicted output to be closer to the target output during the next forward iteration. Thus, it minimises the error for each output neuron and the network as a whole. This process cycle is repeated based on the preset parameter and achieves a certain degree of performance for the classifier.

4.6. Performance Metrics

In machine learning for classification models, the confusion matrix is the typical matrix used for performance indicators such as accuracy, specificity and sensitivity to evaluate the performance of the trained classifiers.

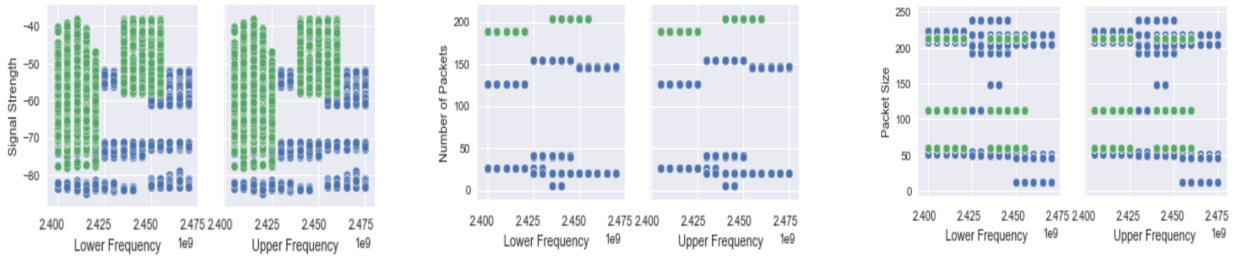
Accuracy performance indicator evaluates the overall performance of the models. The sensitivity performance indicator is the ratio of correctly predicted drone observations to all observations in actual class for the drone class while specificity performance indicator is the ratio of correctly predicted standard Wi-Fi devices observations to all observations in the actual class of Wi-Fi devices. In this paper, these indicators were used to evaluate how well the classifiers has achieved to accurately detect and classify both Wi-Fi drone and standard Wi-Fi devices. Hence, the objective is to achieve a high percentage for these performance indicators when training and evaluating the ML classifiers.

5. RESULTS AND ANALYSIS

In this section, an example of the Wi-Fi drone and standard Wi-Fi devices prediction will be elaborated, followed by an evaluation of the prediction performance using our proposed approach that leverages on the RF and network measurements jointly. Lastly, the performance of the two trained models LR and ANN will be compared.

5.1. Prediction Example

Before training the classifiers, the data set was inspected, and features contained in the file was compared against one another to identify certain patterns and relations through the use of data visualisation.



(a) Frequency Range against RSS

(b) Frequency Range against Number of Network Packets

(c) Frequency Range against Network Packet Size

Figure 8: Data Visualisation

Figure 8 illustrates the scatterplots of the data characteristics of the collected RF and network measurements. The green plotted data belongs to the drone data, and the blue belongs to the standard Wi-Fi devices. Figure 8(a) illustrates the plot on the frequency range versus the signal strength. It shows that there is a distinct RSS signature difference between Wi-Fi drone and standard Wi-Fi devices. The characteristic of a standard stationary Wi-Fi device such as a Wi-Fi access-point displays a uniform signature throughout the captured timeframe. Hence, if using a spectrum analyzer for drone detection, these readings would always be captured at a relatively low RSS reading due to the distance away from the SDR. Fig 8(b) and Fig 8(c) inspect the network characteristics trends. The findings in these data visualisation show a reasonably distinct separation between the two classes. Hence, the findings from figure 8 could presume three following conditions:

- RSS of WI-Fi drone fluctuates overtime.
- Number of packets transmitted by Wi-Fi drone is more than standard Wi-Fi Devices
- Majority of the transmitted packet size of Wi-Fi drone is relatively larger.

and these conditions indicate high probability of drone presence in an area.

5.2. Prediction Performance

With the proposed methodology in the pre-processing of the data and the training schemes for the ML classifiers, a significant improvement in training performance indicators over existing methodology has been achieved with 100% in the respective performance indicators for both classifiers is shown in table 1 below. The classifiers models were finalized and were used to predict with the

Performance Indicators	LR	ANN
Accuracy	100%	100%
Sensitivity	100%	100%
Specificity	100%	100%

Table 1: Classifier's Performance With SKFCV and GSCV for ANN

testing data. As shown in table 2, the performance of the test results was illustrated for each classifier.

Both LR and ANN classifiers were able to obtain good accuracy rate of 89.8% and 95% respectively, which shows good overall performance for differentiating the two classes. To further inspect

Performance Indicators	LR	ANN
Accuracy	89.8%	95%
Sensitivity	100%	100%
Specificity	87.6%	93.9%

Table 2: Classifier's Performance With Unseen Test Data

into the specific details of the classifiers performance, sensitivity and specificity readings were observed. Both classifiers have achieved 100% sensitivity rate and obtained specificity of 87.6% and 93.9% for LR and ANN classifiers respectively. The results of the performance of both classifiers have shown that with the joint use of specific RF and network signatures, the trained classifiers were able to predict the presence of Wi-Fi drone accurately based on sensitivity performance indicator. However, based on the specificity indicator, the classifiers have made a slight error in mistaken the standard Wi-Fi devices as Wi-Fi drone, but overall it has achieved relatively good results in identifying a standard Wi-Fi device with high specificity rate.

5.3. Classifiers Comparison and Implementation Remarks

Performance Indicators	RF and Network Measurements		RF Measurements	
Classifiers	LR	ANN	LR	ANN
Accuracy	89.8%	95%	74.7%	73.37%
Sensitivity	100%	100%	4.5%	7.51%
Specificity	87.6%	93.9%	99%	96%

Table 3: Classifier's Performance Using Different Measurements

Table 3 shows a comparison performance result of each classifier with different type of measurement data. The ANN classifier has displayed better performance than the LR, in having a lower false positive value, making lesser error predictions in predicting standard Wi-Fi devices as drones. Although LR classifier may not perform as good as the ANN classifier, the simplex LR classifier could be an effective and efficient classifier in detecting specific drones model and Wi-Fi environment as the performance results do not differ very far from the ANN classifier performance. The trained results have proved that with the joint use of both RF and network measurements, it could outperform the classifiers that uses standalone RF measurements.

However, in the real world scenario, many different types of drone models transmit different data measurements. Thus, a need of a complex classifier like ANN should be utilized as the drone detection classifier since it could analyze and detect the underlying trend of different drone data characteristics, and produce a good detection accuracy. Thus, the selection of the classifier could be based on the environment condition to determine the need for a simplex or a complex classifier to be deployed as drone detection application.

In our proposed approach, the Wi-Fi drone detection is based on the captured timeframe of the RF and network measurements, and within the range of SDR. In order to reduce the false positive rate and improve the performance of the classifiers, more drones can be deployed during the data collection phase. One straightforward method is to have a sufficient amount of drones to cover the whole Wi-Fi RF spectrum so that the data collected would have the drone characteristics in whole Wi-Fi spectrum and the classifier would be able to predict if there is a sudden appearance of a Wi-Fi drone in the area. Another method would be using more SDRs to ensure better coverage of the whole environment and collect more accurate measurements.

6. CONCLUSION

This paper proposes a novel machine learning approach to identify Wi-Fi drones in a dense Wi-Fi environment with both RF and network measurements. Instead of using high cost and sophisticated equipment to decode the transmitted RF signals to identify a drone presence, our simple and yet cost-effective proposed approach is sufficient to detect a drone presence by observing both RF and network measurement trends jointly. Two machine learning classifiers, LR and ANN ML

models were trained under the proposed meticulous preparation and procedures, and have displayed good performance results in achieving 100% accuracy in detecting Wi-Fi drones in a dense Wi-Fi environment. It has been shown experimentally that using both RF and network measurements jointly could outperform existing methodology that only utilize single measurements by 15.1% and 21.63% respectively.

In this paper, our trained classifier was able to show good performance in detecting Wi-Fi drone based on model-Mavic Air. However, different drone models may transmit different types of network characteristics.Hence, future work will be considered in testing the trained classifier using collected data from different drone models to evaluate the classifier ability to detect other drone models or network devices under different dense Wi-Fi environment. In addition, more different types of popular drone models and network devices could be employed to train the classifier and cover the whole Wi-Fi spectrum, so that the classifier would be able to detect drone presence at any crowded Wi-Fi environment conditions accurately in hoping to achieve the deployment of this classifier for drone detection.

REFERENCES

1. Zhang RenYu, Seow Chee Kiat, Wen Kai, and Zhang Heng, "Spoofing Attack of Drone",*2018 4th IEEE International Conference on Computer and Communications (ICCC)*, pp. 1239-1246, Dec 2018.
2. M. Donatti, F. Frazatto, L. Manera, T. Teramoto, and E. Neger, "Radio frequency spoofing system to take over law-breaking drones," *in 2016 IEEE MTT-S Latin America Microwave Conference (LAMC)* , Puerto Vallarta, Mexico, 2016, pp. 13.
3. W. D. Scheller, "Detecting drones using machine learning," Iowa State University, United States, 2017.
4. Phuc Nguyen, Mahesh Ravindranathan, Anh Nguyen, Richard Han and Tam Vu, "Investigating Cost-effective RF-based Detection of Drones", *The 14th ACM International Conference on Mobile Systems, Applications, and Services Singapore*, pp. 17-22, 2016.
5. Nguyen, H. Truong, M. Ravindranathan, A. Nguyen, R. Han, and T. Vu, "Matthan: Drone Presence Detection by Identifying Physical Signatures in the Drones RF Communication,"*in Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys 17*, Niagara Falls, New York, USA, 2017, pp. 211224.
6. C.K. Seow and S.Y. Tan, "Localization of Omni-Directional Mobile Device In Multipath Environments," *Progress in Electromagnetics Research*, Vol.85, pp. 323-348, 2008.
7. S.W. Chen, S.Y. Tan, and C.K. Seow, "Peer-to-peer localization in urban and indoor environments," *Progress in Electromagnetics Research B*, Vol. 33, pp. 339-358, 2011 .
8. H. Zhang, C.K. Seow, and S.Y. Tan, "Virtual Reference Device-Based Narrowband TOA Localization using LOS and NLOS path,"*2016 IEEE/ION Position, Location and Navigation Symposium (PLANS16)*, Savannah, GA, Apr. 11-14, 2016, pp.225-231.
9. C.K. Seow and S.Y. Tan, "Non-Line-of-Sight Unidirectional Mobile localisation in Multipath Environment",*Electronics Letters*, Vol. 44, Issue 2, pp.141-142, Jan. 2008.
10. I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, "Unauthorized Amateur UAV Detection Based on WiFi Statistical Fingerprint Analysis," *IEEE Communications Magazine*, vol. 56, no. 4, pp. 106111, Apr. 2018.
11. P. Kosolyudhthasarn, V. Visoottiviseth, D. Fall, and S. Kashihara, "Drone Detection and Identification by Using Packet Length Signature,"*in 2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, Nakhonpathom, Thailand, 2018, pp. 16.
12. S. Dreiseitl and L. Ohno-Machado, "Logistic regression and artificial neural network classification models: a methodology review,"*Journal of Biomedical Informatics*, vol. 35, no. 56, pp. 352359, Oct. 2002.
13. C. A. Ramezan, T. A. Warner, and A. E. Maxwell, "Evaluation of Sampling and Cross-Validation Tuning Strategies for Regional-Scale Machine Learning Classification," Remote Sensing, vol. 11, no. 2, p. 185, Jan. 2019.
14. C. Nwankpa, W. Ijomah, A. Gachagan, and S. Marshall, "Activation Functions: Comparison of trends in Practice and Research for Deep Learning," arXiv:1811.03378 [cs], Nov. 2018.